REMARKS

This communication is responsive to the non-final Office Action mailed August 22, 2008 and also to the telephonic interview conducted on Tuesday, November 25, 2008.

Examiner Interview Summary

Applicant appreciates the time taken by Examiner Kane to have a telephonic interview with the undersigned and with inventor Peter Avritch. During the interview, no exhibits were shown.

The discussion centered around claim 1 and the Mulder reference, which is a secondary reference applied in an obviousness rejection. The Montville primary reference was also generally discussed.

No agreement was reached.

Claim Rejections – 35 USC § 103

Claims 1, 2, 4, 9, 10, 12-17, 19-24, 35 and 36 are rejected as being obvious over Montville, in view of Mulder. For at least the reasons set forth below, Applicant respectfully traverses the rejection.

In the first place, even if Montville was modified in view of Mulder to include a "service key," as the Examiner terms the MEK described at [0024] of Mulder, this still does not yield the recited subject matter, since the MEK is not a "service private key" as recited in the rejected claims.[1]

More particularly, Mulder recognizes the difficulty of recipients that are "smaller entities" to keep track of public keys of senders. As disclosed by Mulder at [0006],

> Thus, the system of the present invention may be advantageously implemented for sending secure e-mail from one large entity to many smaller entities. The information thus sent is encrypted using advanced encryption algorithms that guarantee privacy within the limits of existing technology. The generation and upkeep of the key pairs is the responsibility of the larger entity (sender).

[1] In fact, when this was pointed out to the Examiner during the telephonic interview, even the Examiner recognized this shortcoming, stating (which may be a paraphrase) "I said Mulder discloses a 'service key,' not a 'service private key.'"

Thus, as described at [0024] of Mulder cited by the Examiner and also at [0028] of Mulder, a secure delivery service employs a symmetric algorithm to generate the MEK and encrypt content, provided from a sender, using the MEK. (Again, it is noted that the MEK is not a "service private key.") A key agreement algorithm is used to wrap the MEK for delivery to the recipient, for use by the recipient to decrypt the encrypted content. The recipient's public key and the sender's private key are used to create a shared secret to wrap the MEK. Yet further, a JAR file is created to include decryption algorithm code, key agreement algorithm code, the wrapped MEK, the sender's public key, the encrypted content, and other information. The JAR file is signed using the sender's private key.

The MEK is not a "service private key," nor is there anything else in Mulder that discloses or suggests any other key that could be considered a "service private key." For this reason alone, the modification of Montville in view of Mulder to include generation and use of an MEK is insufficient as a basis for an obviousness rejection of claim 1.

Furthermore, the Examiner's stated motivation for modifying Montville in view of Mulder is insufficient in any event. The Examiner states "The suggestion/motivation for doing so would have been reduced involvement and effort of the recipient in order to receive and view the secure information (page 1, paragraph 6)." However, given the intricate series of steps disclosed by Mulder to facilitate transmission of data securely from a sender to a recipient, it is not even clear what modification one of ordinary skill in the art would be motivated to make to Montville in view of Mulder. More logically, it would appear that given the intricate series of steps disclosed by Mulder, one of ordinary skill in the art would not be motivated to modify Montville or any reference in view of Mulder. In fact, perhaps, rather than modifying the Montville system in view of Mulder, it may be more sensible to use the Mulder system in place of the Montville system.

We now discuss the Examiner's contention, during the telephonic interview but not contained at all in the Office Action, that one of ordinary skill in the art would be motivated to replace the MEK of Mulder with a "service private key" as recited in the claims. In the first place, if the Examiner intends to rely on such a contention in rejecting the claims, then the contention should be in writing. Furthermore, even during the telephonic interview when this contention was made, the Examiner was unable to provide any support for this contention. As best understood by Applicant's undersigned attorney, though, the Examiner seemed to be contending (again, without being able to point to any support for the contention) that the

public/private key asymmetric scheme and a symmetric MEK scheme are essentially interchangeable.

In the interest of advancing prosecution, Applicant undertakes to rebut what is thought to be the Examiner's contention, that a public/private key asymmetric scheme and a symmetric MEK scheme are essentially interchangeable. For example, Applicant refers the Examiner to the book "Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C" by Bruce Schneier (Wiley Computer Publishing, John Wiley & Sons, Inc. 1996). The Schneier reference is a highly-regarded general authority on cryptography. Referring to section 10.2, in a section entitled "Public-Key Cryptography versus Symmetric Cryptography," the author writes:

> Which is better, public-key cryptography or symmetric cryptography? This question doesn't make any sense, but has been debated since public-key cryptography was invented. The debate assumes that the two types of cryptography can be compared on an equal footing. They can't.
>
> Needham and Schroeder [1159] pointed out that the number and length of messages are far greater with public-key algorithms than with symmetric algorithms. Their conclusion was that the symmetric algorithm was more efficient than the public-key algorithm. While true, this analysis overlooks the significant security benefits of public-key cryptography.
>
> Whitfield Diffie writes [492,494]:
>
> > In viewing public-key cryptography as a new form of cryptosystem rather than a new form of key management, I set the stage for criticism on grounds of both security and performance. Opponents were quick to point out that the RSA system ran about one-thousandth as fast as DES and required keys about ten times as large. Although it had been obvious from the beginning that the use of public key systems could be limited to exchanging keys for conventional [symmetric] cryptography, it was not immediately clear that this was necessary. In this context, the proposal to build hybrid systems [879] was hailed as a discovery in its own right.
>
> Public-key cryptography and symmetric cryptography are different sorts of animals; they solve different sorts of problems. Symmetric cryptography is best for encrypting data. It is orders of magnitude faster and is not susceptible to chosen-ciphertext attacks. Public-key cryptography can do things that symmetric cryptography can't; it is best for key management and a myriad of protocols discussed in Part I.
>
> Other primitives were discussed in Part I: one-way hash functions, message authentication codes, and so on. Table 10.1 lists different types of algorithms and their properties [804].

Further, as best understood by Applicant, the Examiner seemed to be contending during the telephonic interview that public/private key cryptography is more secure than symmetric key cryptography, which would lead one of ordinary skill in the art to substitute public/private key

cryptography for the symmetric MEK of Mulder. Generally, as discussed by Schneier, public-key encryption may in fact be less secure and less efficient than symmetric key cryptography.

For example, Schneier also notes, at section 2.6, entitled "Digital Signatures":

> In practical implementations, public-key algorithms are often too inefficient to sign long documents. To save time, digital signature protocols are often implemented with one-way hash functions [432,433]. Instead of signing a document, Alice signs the hash of the document. In this protocol, both the one-way hash function and the digital signature algorithm are agreed upon beforehand.

Furthermore, in Chapter 19, Public-Key Algorithms, Schneier further states:

> 19.1 Background
>
> The concept of public-key cryptography was invented by Whitfield Diffie and Martin Hellman, and independently by Ralph Merkle. Their contribution to cryptography was the notion that keys could come in pairs—an encryption key and a decryption key—and that it could be infeasible to generate one key from the other (see Section 2.5). Diffie and Hellman first presented this concept at the 1976 National Computer Conference [495]; a few months later, their seminal paper "New Directions in Cryptography" was published [496]. (Due to a glacial publishing process, Merkle's first contribution to the field didn't appear until 1978 [1064].)
>
> Since 1976, numerous public-key cryptography algorithms have been proposed. Many of these are insecure. Of those still considered secure, many are impractical. Either they have too large a key or the ciphertext is much larger than the plaintext.
>
> Only a few algorithms are both secure and practical. These algorithms are generally based on one of the hard problems discussed in Section 11.2. Of these secure and practical public-key algorithms, some are only suitable for key distribution. Others are suitable for encryption (and by extension for key distribution). Still others are only useful for digital signatures. Only three algorithms work well for both encryption and digital signatures: RSA, ElGamal, and Rabin. All of these algorithms are slow. They encrypt and decrypt data much more slowly than symmetric algorithms; usually that's too slow to support bulk data encryption.
>
> Hybrid cryptosystems (see Section 2.5) speed things up: A symmetric algorithm with a random session key is used to encrypt the message, and a public-key algorithm is used to encrypt the random session key.

Interestingly, it is noted that the statement immediately above regarding "Hybrid cryptosystems" appears to at least partially describe the type of system disclosed by Mulder (i.e., except for the Mulder JAR, which includes the decryption algorithm and the key agreement algorithm).

Claims 5-7 are rejected as being unpatentable over Montville in view of Mulder and further in view of Zoken. Claims 5-7 are related to taking an action based on an outcome of assessing the integrity of a message. Notably, the email inbox organization in Zoken has nothing to do with assessing the integrity of a message, and particularly has nothing at all to do with processing a result-incorporated e-mail message using a public key (let alone a service public

key) to assess the integrity of an email message. The Examiner contends a motivation for modifying Montville in view of Mulder to include performing an action based on "the integrity assessment of Zoken" would have been "to treat similarly certified documents the same." The Examiner does not provide any support, however, for this alleged motivation. Even under the KSR case, the Examiner is not permitted to make bald assertions of obviousness and/or motivation without support. For example, the Examiner has not shown that the alleged modification yields predictable results.

Claims 25, 26 and 31-34 are rejected as being obvious over Montville in view of Mulder in view of McKeon. Claims 27-30 and 44-46 are rejected as being obvious over Montville in view of Mulder and further in view of Heiner. Claims 38-40, 42 and 43 are rejected as being obvious over Montville in view of Mulder and further in view of Castell. Claims 47-49 are rejected as being obvious over Montville in view of Mulder and further in view of Morkel.

In each case, the rejected claims are patentable for at least the reasons claims 1, 2, 4, 9, 10, 12-17, 19-24, 35 and 36 are patentable over Montville in view of Mulder, as discussed in great detail above. In addition, the Examiner's alleged motivations for combining the various cited references are deficient because they employ impermissible hindsight reasoning, without the support required by, for example, the KSR case, such as a teaching, suggestion or motivation to make the modification or other permissible principle of obviousness.

CONCLUSION

It is respectfully submitted that Montville in view of Mulder does not yield what is recited in the claims against which that combination is cited. In addition, it is submitted that the Examiner's statement during the telephonic interview regarding the alleged interchangeability of symmetric and asymmetric keys is not only procedurally improper, but is also substantively incorrect. Finally, it is respectfully submitted that the combination of Montville, Mulder and Zoken does not yield what is recited in the claims against which that combination is cited, nor is the alleged motivation to combine proper in any event.

Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,
BEYER LAW GROUP LLP

/ASH/
Alan S. Hodes
Reg. No. 38,185

P.O. Box 1687
Cupertino, CA 95015-1687
408-255-8001